

Rec'd PCT/PTO

10 DEC 2004

10/12/428

PCT/IB2003/002425

PATENT COOPERATION TREATY



Translation

## PCT

## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference P-14-418-PCT	<b>FOR FURTHER ACTION</b> See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/IB2003/002425	International filing date (day/month/year) 10 June 2003 (10.06.2003)	Priority date (day/month/year) 12 June 2002 (12.06.2002)
International Patent Classification (IPC) or national classification and IPC H04L 9/08, H04N 7/16		
Applicant NAGRACARD SA		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 4 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of \_\_\_\_\_ sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 20 December 2003 (20.12.2003)	Date of completion of this report 07 June 2004 (07.06.2004)
Name and mailing address of the IPEA/EP P.B. 5818 Patentlaan 2/ NL-2280 HV Rijswijk Tel. +31 70 340-2040 Facsimile No. +31 70 340-3016	Authorized officer Holper, G Telephone No. +31 70 340-2304

PCT/IB2003/002425

1. This report has been drawn on the basis of (Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.);

- 2. The amendments have resulted in the cancellation of:**

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

**BEST AVAILABLE COPY**

## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

Intern application No.  
PCT/IB 03/02425

## V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

## 1. Statement

Novelty (N)	Claims	1-16	YES
	Claims		NO
Inventive step (IS)	Claims	1-16	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-16	YES
	Claims		NO

## 2. Citations and explanations

Reference is made to the following document:

D1: WO 97/38530 (DIGCO)

The present application relates to a method for securely exchanging data between two locally mutually connected devices and a receiver for implementing said method.

The closest prior art is D1, which discloses a method for securely exchanging data between a receiver and a security module, wherein the two devices are locally connected. The receiver comprises a public key whereas the security module comprises a corresponding private key. The method is used for exchanging a random session key encrypted by means of the public key.

In the prior art, a problem arises in that an intruder can force the session key and thereby exploit a lack of security of the method.

According to claim 1, this problem is solved by the steps of generating a different random number in each device, encrypting this number by means of the first and second keys of the pair of keys respectively, transmitting the

encrypted number to the other device, decrypting the numbers encrypted in each device and combining said random numbers to generate a session key used for exchanging data between the two devices.

A method based on the encryption of two random numbers encrypted by means of two separate keys from the same pair of keys is neither known from, nor suggested by, the prior art. Claim 1 therefore meets the requirements of novelty and inventive step of PCT Article 33(2) and (3).

The receiver according to claim 15 is used for implementing the method according to claim 1 and therefore also meets the requirements of novelty and inventive step.

The additional features of dependent claims 2 to 14 and 16 define details of the embodiment of the invention; said claims are therefore also novel and inventive.

The claimed methods and receivers are industrially applicable.

**BEST AVAILABLE COPY**